

Probleemoplossing voor Secure Access Error "a;VPN-vestigingsmogelijkheid voor een externe gebruiker is uitgeschakeld. Er wordt geen VPN-verbinding tot stand gebracht"a ingesteld.

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

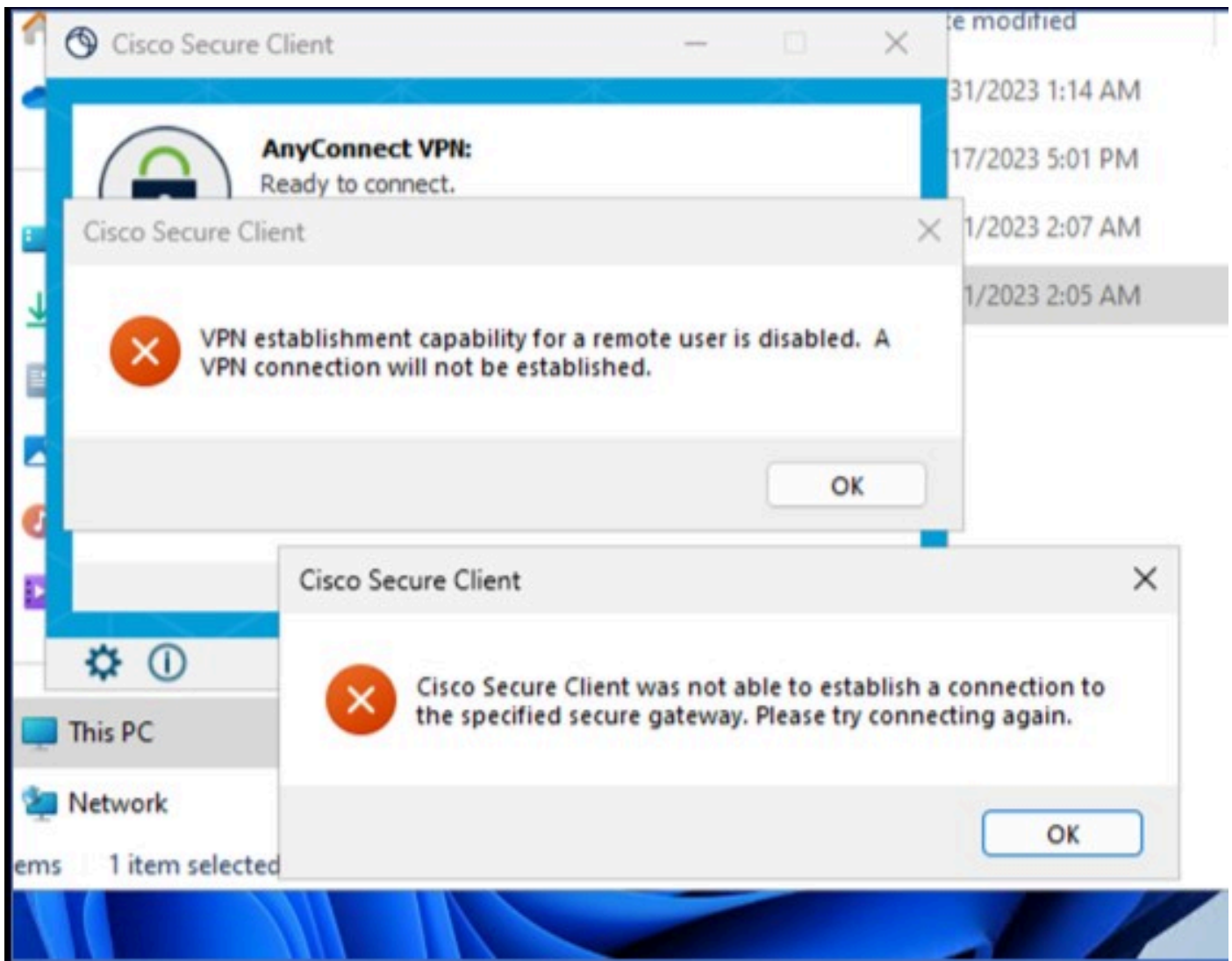
Inleiding

Dit document beschrijft hoe u een fout kunt oplossen: "De VPN-vestigingsmogelijkheid voor een externe gebruiker is uitgeschakeld. Er wordt geen VPN-verbinding tot stand gebracht."

Probleem

Wanneer een gebruiker probeert verbinding te maken met RA-VPN (Remote Access VPN) met de Secure Access-head-end, wordt de fout afgedrukt in het venster voor beveiligde clientmelding van Cisco:

- VPN-vestigingsmogelijkheid voor een externe gebruiker is uitgeschakeld. A VPN connection will not be established.
- Cisco Secure-client kan geen verbinding met de opgegeven beveiligde gateway maken. Probeer het opnieuw.



Cisco Secure Client - probleem bij verbinding met Cisco Secure Access

De genoemde fout wordt gegenereerd wanneer de gebruiker via de RDP is verbonden met de Windows-pc, probeert verbinding te maken met RA-VPN vanaf de betreffende pc, en **WindowsVPN Establishment** is ingesteld op **Local Users Only** (default option).

Windows VPN Establishment bepaalt het gedrag van de beveiligde client-Cisco wanneer een gebruiker die op afstand is aangemeld bij de client-pc een VPN-verbinding tot stand brengt. De mogelijke waarden zijn:

- **Local Users Only**

Verhindert een op afstand ingelogde (RDP) gebruiker een VPN-verbinding te maken.

- **Allow Remote Users**

Hiermee kunnen externe gebruikers een VPN-verbinding tot stand brengen. Als de ingestelde VPN-verbinding routing echter tot gevolg heeft dat de externe gebruiker wordt losgekoppeld, wordt de VPN-verbinding beëindigd om de externe gebruiker in staat te stellen weer toegang te krijgen tot de client-pc. Externe gebruikers moeten 90 seconden wachten na de oprichting van VPN als ze hun externe inlogsessie willen loskoppelen zonder dat de VPN-verbinding wordt beëindigd.

Oplossing

Navigeer naar Cisco Secure Access Dashboard.

- Klik op **Connect > End User Connectivity**
- Klik op **Virtual Private Network**
- Kies het profiel dat u wilt wijzigen en klik op **Edit**

VPN Profiles
A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

New Service Provider Certificate
Download the new service provider certificate and upload in your identity provider (IdP) to avoid user Authentication failures. The certificate will expire on date 11/8/2023. Download and update the certificate now from [Certificate Management](#)

Q Search + Add

| name | General | Authentication | Traffic Steering | Secure Client Configuration | Profile URL | Download XML |
|------------|---------------------------|----------------|--|-----------------------------|-----------------------------------|------------------------------|
| CiscoSSPT1 | ciscossp1es TLS, IKEv2 | SAML | Connect to Secure Access 1 Exception(s) | 12 Settings | fb57.vpn.sse.cisco.com/CiscoSSPT1 | Download XML |

Edit
Duplicate
Delete

Cisco Secure Access - PRI-VPN

Klik op **Cisco Secure Client Configuration > Client Settings > Edit**

← End User Connectivity
VPN Profile

General settings
Default Domain: ciscossp1es | DNS Server: Umbrella (208.67.222.222, 208.67.222.220) | Protocol: TLS / DTLS, IKEv2

Authentication
SAML

Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions

Cisco Secure Client Configuration 1

Cisco Secure Client Configuration
Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings 3 **Client Settings 12** 2 Client Certificate Settings 4 [Download XML](#)

Pre Selected Settings

- Use Start before Logon: Enabled
- Minimize on connect: Enabled
- Autoreconnect: Enabled
- Windows Logon Enforcement: Single Local Logon
- Linux Logon Enforcement: Single Local Logon
- Windows VPN Establishment: All Remote Users
- Linux VPN Establishment: Local Users Only
- Clear SmartCard PIN: Enabled
- IP Protocol Supported: IPv4
- Proxy Settings: Native
- Allow local proxy connections: Enabled
- Authentication Timeout: 30

Edit 3

Cancel Back Save

Cisco Secure Access - RA-VPN-clientconfiguratie

Klik op **Administrator Settings** en **wijzigen** **Windows VPN Establishment** van **Local User Only** in **All Remote Users**

BEFORE

AFTER

| BEFORE | | AFTER | |
|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| Administrator Settings | | | |
| Windows Logon Enforcement | Windows VPN Establishment | Windows Logon Enforcement | Windows VPN Establishment |
| Single Local Logon | Local Users Only | Single Local Logon | All Remote Users |
| Linux Logon Enforcement | Linux VPN Establishment | Linux Logon Enforcement | Linux VPN Establishment |
| Single Local Logon | Local Users Only | Single Local Logon | Local Users Only |

Cisco Secure Access - Windows VPN-instelling

En klik op Opslaan

Client Settings

General 3

Administrator Settings 9

| | |
|----------------------------------|----------------------------------|
| Windows Logon Enforcement | Windows VPN Establishment |
| Single Local Logon | All Remote Users |
| Linux Logon Enforcement | Linux VPN Establishment |
| Single Local Logon | Local Users Only |

Clear SmartCard PIN User controllable

IP Protocol Supported

IPv4

Proxy Settings

Native

Allow local proxy connections User controllable

Allow optimal gateway selection

Cancel **Save**


Cisco Secure Access - Windows VPN-instelling 2

Wanneer u de RA-VPN-sessie vanaf de externe Windows-pc instelt, moet u de Tunnel Mode als Bypass Secure Access. Anders loopt u het risico de toegang tot de externe Windows-pc te verliezen.

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#) 

Tunnel Mode

Bypass Secure Access 

All traffic is steered outside the tunnel.



Cisco Secure Access - tunnelmodus

Voor meer informatie over Tunnel Mode check het volgende artikel punt nummer 6:

<https://docs.sse.cisco.com/sse-user-guide/docs/add-vpn-profiles>

Gerelateerde informatie

- [Gebruikershandleiding voor beveiligde toegang](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.